COMMENTARY

PUBLIC SAFETY AND NATIONAL SECURITY IMPLICATIONS OF THE HORSEPOX STUDY

Jennifer Snow and James Giordano

THE BIOSECURITY AND counterproliferation communities have been tracking developments in dual-use synthetic biology with growing concern, as such developments may facilitate the creation of agents that pose risks and threats to public safety and national security as a consequence of inadvertent dissemination or intentional use as bioweapons.¹⁻⁵ In this light, the recent paper by Noyce et al⁶ describing how to create a horsepox vaccine from synthesized DNA raises what we believe to be profound ethical and national security questions—and disquiet. Specifically, we express our unease regarding the risks associated with the publication of research that could enable the development and deployment of synthetic bioagents by non-state actors. The authors' methods, while requiring defined laboratory skills, would enable individuals with such ability and access to laboratory resources—including those operating in the do-it-yourself (DIY)/bio-hacker community and/or non-state actors with malicious intent—to leverage new synthetic biology tools to overcome specific barriers and to produce a synthetic orthopoxvirus.

This research could be viewed in a positive light in that it has taken contemporary biosecurity across a key threshold by driving conversations regarding concern for such potential threats into calls for action. The tools and techniques identified by Noyce and colleagues⁶ serve to illustrate the

risks inherent in such work, and the article's publication has prompted the biosecurity community to examine the variety of outcomes (ie, from benign to malevolent) that could result from poorly regulated or unregulated enterprises in synthetic biology. The development of a new variant of vaccine is somewhat perplexing, as many experts have articulated that there was no legitimate need for this line of inquiry, as viable solutions already exist.^{7,8} While the expressed intent of this research was to develop a new live vaccine strain, a key consideration should have been to first examine if, how, and to what extent such dual-use research was in the best interest of global security and public health.

To be sure, the current lack of policy, as well as poorly defined ethical guidelines for the development of synthetically created pathogens, could enable other experimentation that could result in the production of dual-use, dangerous products. New techniques and technologies, and decreased costs of these tools, reduce extant barriers to creating hazardous agents, modifying existing organisms (to increase their morbidity or lethality), and creating pathogens anew.^{2,3} We view this as a clear and present threat and, in response, propose that a formal international body convene (eg, a new Asilomar Convention or the Biological Toxins and Weapons Convention, BTWC) to address the need to revisit and revise classification, standards, ethics, and policy to stay apace with iterative technologic advances.^{2,4}

Jennifer Snow, MS, is a lieutenant colonel in the US Air Force, assigned as the US Special Operations Command Donovan Group Innovation Officer, and USSOCOM J5 Future Plans and Strategy Team Air Force Representative at MacDill AFB; she is the Technology Liaison Officer for SOFWERX, Tampa, FL. James Giordano, PhD, is Professor, Departments of Neurology and Biochemistry, and Chief, Neuroethics Studies Program, Georgetown University Medical Center, Washington, DC, and is the Executive Director, Center for Policy on Emerging Technologies, an international think tank based in Washington, DC.

While we are encouraged by the US Federal Bureau of Investigation's (FBI) ongoing engagement with the domestic DIY/biohacker community,⁹ we believe that additional efforts in engaging biotechnology industries, academic institutions, and other governments conducting synthetic biology research and development may be required. Toward such ends, we propose that other agencies of the US government (eg, National Security Agency, Defense Intelligence Agency, Department of Defense, Department of State, Federal Emergency Management Agency, Centers for Disease Control and Prevention) and their allied partners (eg, Interpol) should identify and specify the risk and threat posed by these emerging technologies, and review existing policies, practices, and tools to ensure adequate identification, surveillance, and control of newly modified or created bioagents. Key areas of focus might include methods and tools that use 3D printing and gene editing that can be easily obtained in the public sector and that can be used to create agents that incur defined biosecurity risks. Simply having analysts look for signatures typical of industrial or nation state weapon sites consisting of full manufacturing lines, specific supplies, specific facilities, and the like is probably no longer realistic, viable, or of value if and when complex components and dangerous agents can be produced by a single individual with necessary knowledge and skills who is able to leverage tools that can be easily acquired at relatively low cost.⁵

The review and application of regulatory measures should be thoughtful and must consider how to control risk and threat without excessively limiting beneficial aspects of the technology that can be important to medicine when responsibly engaged. This will require a proactive approach that encourages ethical use yet also provides for the fact that not all users will comply with ethics and standards—and some groups will actively seek opportunities for nefarious employment. Risk mitigation will require a shared effort that equally, transparently, and collaboratively involves all participants so as to emphasize that innovation and technology drivers in biosecurity are kept at the forefront of risk and policy discussions.

In many ways, the government lacks the capacity and expertise to be proactive in such oversight. In light of this, we recommend a hybrid approach that combines academic, DIY, and industry experts to inform and advise policy development. Such an approach would enable reporting and feedback from public and private sectors to augment existing government information channels and provide additional expertise and access into communities the government typically cannot reach. This would result in the development of a collaborative, multi-community perspective on—and responsibility for—biosecurity.

An example of this type of shared effort can be seen in the responsible disclosure mechanisms supported by ethical hackers around the globe who identify and report vulnerabilities in digital systems to prevent damaging attacks on government, medical, electrical, economic, and other crit-

ical infrastructure. These private citizens team with government, security researchers, and industry to create a collaborative network that helps to proactively identify and address threats before they become a larger problem. They also work to inform policy and guide regulation regarding cyber capabilities. As noted above, similar, albeit nascent, collaboration already exists in the United States among the biohacker community, federal law enforcement, and the research community, and we advocate its expansion and fortification so as to provide ongoing information and support to biosecurity policy and regulation.¹⁰

We conclude with our reiteration that a formal body such as the BTWC should convene to address the challenges, responsibilities, and opportunities of revised policy and regulations to meet the realistic risks and threats to international biosecurity that new methods in synthetic biology may obtain. We believe that it is—and will be ever more—imperative to continuously evaluate, track, and define new biological threats if a proactive approach to biodefense is to be established and maintained.^{2,4} As we look to the horizon of probability, possibility, and potential, we see the increasing viability of de novo synthesis of known pathogens and creation of new, designer pathogens, and we urge steps be taken against being woefully unprepared to address this challenge and its consequences.

ACKNOWLEDGMENTS

This work was supported in part by federal funds UL1TR001409 from the National Center for Advancing Translational Sciences (NCATS), National Institutes of Health, through the Clinical and Translational Science Awards Program (CTSA), a trademark of the Department of Health and Human Services, part of the Roadmap Initiative, "Re-Engineering the Clinical Research Enterprise" (JG); the European Union's Horizon 2020 Research and Innovation Programme under grant agreement 720270: HBP SGA1 (JG); the AEHS Foundation Project NeuroHOPE (JG); and by the Austin and Ann O'Malley Distinguished Visiting Chair in Bioethics of Loyola Marymount University (JG). The authors declare that they do not have any conflict(s) of interest and that the views and opinions expressed in this essay are their own and do not necessarily represent those of the funding organizations that support their work.

REFERENCES

1. Giordano J. The neuroweapons threat. *Bull At Sci* 2016; 72(3):1-4.
2. DiEuliis D, Giordano J. Why gene editors like CRISPR/Cas may be a game-changer for neuroweapons. *Health Secur* 2017;15(3):296-302.

3. DiEuliis D, Giordano J. Gene editing using CRISPR/Cas9: implications for dual-use and biosecurity. *Protein Cell* 2017; 15:1-2.
4. Gerstein D, Giordano J. Re-thinking the Biological and Toxin Weapons Convention? *Health Secur* 2017;15(6): 638-641.
5. Snow J. *Entering the Matrix: The Challenge of Regulating Radical Leveling Technologies* [graduate thesis]. Monterey, CA: Naval Postgraduate School; 2015. <http://hdl.handle.net/10945/47874>. Accessed January 30, 2018.
6. Noyce RS, Lederman S, Evans DH. Construction of an infectious horsepox virus vaccine from chemically synthesized DNA fragments. *PLoS ONE* 2018;13(1):e0188453.
7. Kupferschmidt K. A paper showing how to make a smallpox cousin just got published. Critics wonder why. *Science* 2018 Jan 19. www.sciencemag.org/news/2018/01/paper-showing-how-make-smallpox-cousin-just-got-published-critics-wonder-why. Accessed January 29, 2018.
8. Soucheray S. Step-by-step horsepox study stokes dual-use controversy. *CIDRAP News* January 23, 2018. <http://www.cidrap.umn.edu/news-perspective/2018/01/step-step-horsepox-study-stokes-dual-use-controversy>. Accessed January 29, 2018.
9. Wolinsky H. The FBI and biohackers: an unusual relationship: the FBI has had some success reaching out to the DIY biology community in the USA, but European biohackers remain skeptical of the intentions of US law enforcement. *EMBO Rep* 2016;17(6):793-796.
10. Kolkman O. Responsible disclosure from a collaborative security perspective. Internet Society website. February 1, 2017. <https://www.internetsociety.org/blog/2017/02/responsible-disclosure-from-a-collaborative-security-perspective/>. Accessed February 21, 2018.